NAVAL WAR COLLEGE
Newport, R.I.

Denial and Deception--Network-Centric Challenge

by

Kevin N. Kearney
Civilian, DIA

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:

5 February 1999

Dr. Elizabeth McIntyre

Unclassified
Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority: N/A

3. Declassification/Downgrading Schedule: N/A

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: NWC C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):

Denial & Deception—Network-Centric Challenge (U)

9. Personal Authors: Kevin N. Kearney, CIA

10. Type of Report: FINAL

11. Date of Report: 05 Feb 1999

12. Page Count: [redacted] 23

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:
Denial & deception, network-centric warfare, information superiority, sensor denial, sensor deception, decoys, misinformation, speed of command, self-synchronization, networked analysis

15. Abstract: Adversarial denial and deception (D&D) poses a serious challenge to future operational concepts based on perceived informational superiority. An analysis of how D&D may interact in a future network-centric environment demonstrates some inherent vulnerabilities of information technology (IT) based warfighting theory. Operational D&D has continued to keep pace with sensor development and through physical, technical and administrative means will be able to influence sensor-derived information. Once our information is tainted, network-centric's reliance on information dominance will become a vulnerability. Deception will travel at high speeds and effect multiple operational levels due to the networked operational picture provided by network-centric theory. Our dependence on reliable and timely information, if affected by D&D, may lead to ambiguity, misdirection, and/or false security. Network-centric's speed of command will further exasperate D&D's effect by increasing the speed of deception while simultaneously reducing the likely identification of deception through analysis. Our speed and networked precision may also finely hone our operational art to the point of making us predictable and therefore more susceptible to adversarial D&D. The additional network-centric attributes of self-synchronization, platform reduction, and adversarial lock-out will also contribute to our vulnerability to D&D by creating an environment of enemy underestimation and increasing the severity of consequences of friendly action taken under the influence of adversarial D&D. The D&D challenge that network-centric warfighting faces can be addressed through an increased emphasis on the importance of networked analysis. Additionally, future doctrine must reflect a clear understanding of anti-D&D methodologies so that operational commanders of the future are aware of and can plan how to counter D&D when they face it.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-6461

20. Office Symbol: NWC C

Security Classification of This Page Unclassified

Abstract

Adversarial denial and deception (D&D) poses a serious challenge to future operational concepts based on perceived informational superiority. An analysis of how D&D may interact in a future network-centric environment demonstrates some inherent vulnerabilities of information technology (IT) based warfighting theory. Operational D&D has continued to keep pace with sensor development and through physical, technical and administrative means will be able to influence sensor-derived information. Once our information is tainted, network-centric's reliance on information dominance will become a vulnerability. Deception will travel at high speeds and effect multiple operational levels due to the networked operational picture provided by network-centric theory. Our dependence on reliable and timely information, if affected by D&D, may lead to ambiguity, misdirection, and/or false security. Network-centric's speed of command will further exasperate D&D's effect by increasing the speed of deception while simultaneously reducing the likely identification of deception through analysis. Our speed and networked precision may also finely hone our operational art to the point of making us predictable and therefore more susceptible to adversarial D&D. The additional network-centric attributes of self-synchronization, platform reduction, and adversarial lock-out will also contribute to our vulnerability to D&D by creating an environment of enemy underestimation and increasing the severity of consequences of friendly action taken under the influence of adversarial D&D. The D&D challenge that network-centric warfighting faces can be addressed through an increased emphasis on the importance of networked analysis. Additionally, future doctrine must reflect a clear understanding of anti-D&D methodologies so that operational commanders of the future are aware of and can plan how to counter D&D when they face it.

TABLE OF CONTENTS

Abstract.. ii

Table of Contents.. iii

I. Introduction.. 1

II. Relevant Elements of D&D and Network Centric Warfare.................. 1
Operational Denial & Deception.. 2
Physical Means.. 2
Technical Means.. 2
Administrative Means... 3
Network-Centric Warfare... 3

III. Denial & Deception's Challenge to Network Centric Warfare........... 4
Networked Grid of Sensors.. 4
Sensor Denial.. 4
Sensor Deception.. 5
Sophisticated Decoys.. 6
Electromagnetic Deception...................................... 6
Misinformation.. 7
Informational Dominate Battlespace-Common Picture.............. 7
Shared Perceptions--Shared Deception.......................... 8
Information Dominance--Information Dependence......... 8
Ambiguity.. 9
Misdirection... 9
False Security.. 9
Speed of Command... 10
Speed of Deception... 10
Speed vs. Analysis... 10
Predictability of Perfection.. 11
Self-synchronization... 13
Less platforms, more networks... 13
'Lock-out' or Underestimation... 14

IV. Potential Ability of Informational Superiority to overcome D&D..... 14
Role of Networked Analysis... 14
Doctrine... 16

V. Conclusion.. 17

Bibliography.. 19

Denial and Deception -- Network-Centric Challenge

I. Introduction

Adversarial operational denial and deception (D&D) will challenge the assumed premise of future network-centric operational art: information superiority. Denied or altered information will have an increasingly negative impact on operational decision-makers as they become accustomed to the complete battlespace awareness promised by network-centric theory.

The role denial and deception (D&D) has played throughout the history of war is not likely to end with the advent of revolutions in military affairs (RMAs) based on information technology (IT). This paper will look at aspects of the evolving IT RMA (specifically network-centric warfare) and identify inherent attributes that may leave operational decision-makers susceptible to future and inevitably improved enemy D&D methodology. As operational art progresses down the path of true information dominance, D&D will become one of our enemy's last and arguably most cost effective counters to our superiority. The potential soft underbelly of our IT RMA (created by D&D) must be explored early on so that remedies can be programmed into both our operational/intelligence community development and our changing warfare doctrine.

II. Relevant Elements of D&D and Network-Centric Warfare

Sun Tzu saw D&D as the key to achieving surprise and therefore felt that "all warfare is based on deception."[1] While warfare has obviously evolved since the 3rd century BC, current IT RMA theory--namely network-centric warfare--is currently

[1] Michael Handel, Sun Tzu and Clausewitz (Carlisle Barracks: U.S. Army War College 1991), 40.

developing without an appreciation for the destructive potential of future operational D&D. Our technology, if not tailored to deal with this reality, may well blind us to the ancient but still persistent threat of D&D. Understanding the modern relevance of D&D is pivotal to recognizing the potential threat. The interaction between D&D and network-centric warfare will be explored in this paper. Understanding interaction first requires an understanding of the actors so let's begin by briefly introducing both.

Operational Denial & Deception

> *Always mystify and mislead the enemy.*
>
> **General Stonewall Jackson**

JCS defines deception as "those measures designed to mislead enemy forces by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests."[2] While deception alters evidence, denial simply provides no evidence in order to induce the enemy into making an adverse reaction. Denial and deception complement each other in the operational art of shaping perceptions to gain advantage on the battlespace. D&D uses information to influence the adversary's emotions, motives, and objective reasoning. To achieve this, D&D seeks to manipulate decision-makers in order to ultimately produce behaviors and actions favorable to the originator's objectives. There are three main categories of deceptive means:[3]

Physical means--activities and resources used to convey or deny selected information to an adversary (i.e., feint, ruse, demonstration, exercises, training, maneuver, decoys, tactics, bases, logistic actions, stockpiles). In a modern context, physical deception is largely directed at ground sensors and imagery intelligence (IMINT).

Technical means--military resources and associated operating techniques

[2] Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms (Joint Pub 1-02)(Washington: March 23, 1994), 118.

[3] Ibid., 119.

used to convey or deny selected information to an adversary through: deliberate radiation, reradiation, alteration, absorption, or reflection of energy; the emission or suppression of chemical or biological odors; and the emission or suppression of nuclear particles. It is largely directed at signals and measurement & signature intelligence (SIGINT and MASINT).

Administrative means--resources, methods, and techniques to convey or deny oral, pictorial, documentary, or other physical evidence to an adversary. It is largely directed at mass media and human intelligence (HUMINT).

Network-Centric Warfare

> *While the friction and fog of war can never be eliminated, new technology promises to mitigate their impact.*
>
> **Joint Vision 2010**

Network-centric theory is an evolving concept of warfighting that is attempting to give the ongoing IT RMA an identity. Network-centric warfighting involves synchronized and networked warfighting (engagement and sensor) nodes operating at high speeds. Success on the network-centric battlespace will require ***information superiority*** made possible by a ***networked grid of sensors.*** The informational superiority will be networked to create a common battlespace awareness (picture) that will allow for ***speed of command*** and, due to the shared perception, lead to a high degree of ***self-synchronization.*** The nature of network-centric warfare theory supports (and may have the result of encouraging) the current defense environment which is marked by a ***declining number of platforms***. Network-centric warfare theory assumes that if its tenants are fully assimilated into our military's warfighting doctrine that future operational commanders with be able to ***lock out*** enemies by combining speed and self-synchronization on the battlespace.[4]

[4] VADM Arthur Cebrowski and John Garstka, "Network-Centric Warfare--Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 28-35.

III. Denial & Deception's Challenge to Network-Centric Warfare

Networked sensor grids, information superiority, speed of command, self-synchronization, platform devaluation, and assumed adversarial lock-out all combined give many advantages to any possessor of network-centric warfare capabilities, but also all share inherent vulnerabilities to old fashioned (and new fashioned) D&D. The following section will describe how the same attributes that provide strength to network-centric theory will also contribute to modern warfare's continued susceptibility to D&D.

Networked Grid of Sensors

The whole is clearly better than the sum of the parts.

VADM Cebrowski and John Garstka on sensor grids

U.S. multispectural sensor capability (radar, MASINT, SIGINT, IMINT, HUMINT, etc.) is clearly unrivaled and has thus become a critical strength that figures in all of our military warfighting doctrine. Because our sensor grids have become so operationally critical (and will become even more critical under network-centric theory), we can expect future adversarial targeting of these grids. [5]

The redundant and mutually supportive nature of our future sensor grids will make their total defeat or destruction an impracticable endeavor for most future adversaries. A sub-discipline of information warfare--information protection--will argueably be successful in protecting the technical integrity of our sensors. Adversarial targeting of our sensor grids, therefore, will likely focus on denying our sensors information or providing our sensors deceptive information. Potential adversaries have a variety of means at their disposal to achieve this D&D.

Sensor Denial--Signature management, the assessment of and control of one's own vulnerability to sensor technology, has been utilized since WWII.

[5] Milan Vego, On Operational Art-Third Draft (Newport: Naval War College, 1998), 131-144 .

Countermeasure development has consistently followed sensor improvements since WWII. Special netting, paints, coatings, and other camouflage aids are available today that can mitigate visual, near infrared, thermal infrared and radar sensors. A customized and integrated signature management program will combine advanced camouflage, deception techniques (including decoys), mechanical modifications of objects and equipment, adaptation of signatures, and thorough personnel training.

Sensor denying signature management technology is readily available today - as just one example of the numerous international sources, the Swedish company BARRACUDA Technologies AB markets its modern signature management and decoy technology in over 40 nations.[6] Diverse source firms in Greece, UK, US, Italy, Denmark, South Africa, France, and Russia ensure both the wide availability of this technology as well as its continual competitive improvement. Signature management technology's non-lethal/defensive nature makes the export of signature management technology internationally acceptable while relegating its proliferation to the lower tiers of our intelligence collection priorities.

Proliferation of the following technologies will provide our adversaries at least some ability to deny our future sensor grids critical information on the future battlespace: disseminating devices, obscurants, thermal covers/screens, radar-absorbing material/paints, low observable technologies (stealth), and tailored multispectural camouflage devices. These technologies, far from being confined to 'black' superpower programs, are now widely availiable. Many have dual-use applications which have led to commercial developments--a trend that may cloud our perception of the potential operational threat these technologies will pose to us in the future.

Sensor Deception--The more sophisticated our enemy becomes, the more likely it is that they will attempt to combine sensor denial with sensor deception. Even

[6] Iriani Zulkifli, "Company Profile: Barracuda Technologies AB," Asian Defense Journal, Apr 1998, 94.

partial knowledge of our sensor characteristics will allow future adversaries the requisite channels for delivering deception. This potential vulnerability receives decent visibility in Information Warfare circles as we program in protection for network intrusions for deceptive purposes. However, it is at the lower end of the technical spectrum that we may find our sensor grid the most vulnerable.

Old-fashioned deception techniques spiced up with modern capabilities could go a long ways towards downgrading the quality of information generated by our sensor grids. The use of sophisticated decoys (physical deceptive means), electromagnetic deception (technical deceptive means), and the supply of misinformation through human sources (administrative deceptive means) are just three examples of sensor deception that we will look at to illustrate our sensor grids' vulnerability to relatively low-tech deception.

- **Sophisticated decoys--**It is ironic that our vast and redundant resources devoted to imagery intelligence (IMINT) can be deceived by one of warfare's oldest and least advanced deceptions - the use of decoys. IMINT sensor advances have been mirrored by innovations in decoy sophistication. Current signature management technology allows for the creation of decoys that emit signatures (visible, IR, and radar) that emulate platforms (tanks, mobile/fixed missile launchers, communication nodes, etc.). The confusion and possible deception caused by this relatively inexpensive measure could seriously degrade IMINT sensor-derived information. Targeting, battle damage assessment, and enemy order of battle studies would all be negatively effected by any amount of IMINT sensor deception.
- **Electromagnetic deception--**Electromagnetic deception was used extensively and effectively during WWII. It provides the deceiver with a relatively low cost method of clouding their opponent's SIGINT-derived battlespace awareness. Paradoxically, as our SIGINT sensors become more and

more sophisticated, our adversaries will be more likely to be able to plant deception through this route. The introduction of false signals and the creation of deceptive transmission sites/communications nodes may not totally deceive our SIGINT system, but it very well may blur the perception gained from this important sensor. Once blurred, the accuracy of the whole SIGINT sensor grid may be undermined by uncertainty generated by the fear of deception and the noise generated by the deceptive measures themselves.

- Misinformation--Deception is an inherent danger in the world of human espionage and raw HUMINT reporting is supposed to be thoroughly fused with all source intelligence so as not to become an avenue for adversarial deception. As we move away from Cold War espionage, however, we may be becoming lax in our efforts to prevent HUMINT from becoming a vehicle for deception. HUMINT is often the only source of information we have on the adversary's intentions, mindset, and morale. An adversary intent on portraying innocent intentions in place of actual aggression could deceive our HUMINT sources (sensors) by allowing the leakage of misinformation that demonstrates only innocent intentions. On the operational/tactical level, a deceptive adversary could plant misinformation on enemy plans with our tactical level sources and POWs.

Informational Dominate Battlespace--the common operating picture

The D&D vulnerabilities described above could become critical vulnerabilities as they act on network-centric's operational picture. As we seek dominant battlespace awareness, quality of information becomes ever more vital. Network-centric theory relies on the achievement of information superiority to facilitate its deliverables (namely speed and self-synchronization). The content, quality, and timeliness of information moving between nodes on the network has an intrinsic value that increases as information "moves toward 100% relevant content, 100% accuracy, and zero time delay--toward information superiority."[7] This information would feed in from our sensor grids directly (in most cases) into the creation of a common operating picture. This picture would contain complex and diverse information graphically displayed to facilitate rapid dissemination and thereby speed of command.

The common picture will provide decision-makers, their superiors, and their subordinates the current and predicted status of friendly and enemy forces, threats, logistics, weather, sensors, terrain, etc. It will obviously become indispensable--and just as obviously a priority enemy target. As with the sensor grid, much has been done already to program protection into this structure from an informational warfare (protection) standpoint. But the nature of the common operating picture also make it a fertile ground for planting deception. Lets now look at how even a small amount of deception could dangerously damage our operational awareness.

Shared Perceptions/Shared Deception--Operational deception has always targeted the decision-makers with the goal of reinforcing preconceptions and/or tailoring assumptions. Traditional deception had the difficult task of infiltrating numerous leadership echelons each with varying preconceptions and assumptions. The job required precise intelligence and reliable feedback mechanisms to ascertain success. Network-centric's common operating picture will offer one stop shopping to the deceiver of the future. Any concerted effort to deny or deceive our sensor grids will likely be able to affect the common picture and thereby immediately begin to influence our operational art.

Information Dominance/Information Dependence--Denied or deceived intelligence will have a greater negative effect on operational commanders as they

[7] VADM Arthur Cebrowski and John Garstka, "Network-Centric Warfare--Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 31.

become accustomed to near complete battlespace awareness. The uncertainty created by D&D would therefore have an even more detrimental effect on the decisionmaker's mind than in the past.[8] Susceptibility to ambiguity, misdirection, and false security are only three examples of the potential vulnerability this informational dependence will create for the future network-centric decisionmaker.

- **Ambiguity--**Uncertainty has a tremendously destabilizing effect on our thought process. D&D can often inject uncertainty into a decision cycle in such a way that even if the D&D is not believed, the uncertainty can be detrimental to the timeliness and quality of the final decision.[9]
- **Misdirection--**Successful D&D will cause a victim to act, not just continue to seek ground truth. The deceived side proceeds under the impression that their action is decisive based on their pre-existing beliefs that were reinforced by D&D.[10]
- **False Security**--Successful D&D will usually be designed to also provide the commander a false sense of certainty. Our minds are conditioned to believe information that reinforces preconceptions. The tendency is to jump to conclusions once information lines up with our preconceived beliefs.[11] Once an enemy can determine our preconceptions, he will be able to tailor his D&D efforts to reinforce the false ones.

[8] Michael Dewar, The Art of Deception In Warfare, New York, Sterling, 1989, 9.
[9] Ibid.
[10] Bradley Nelson, Battlefield Deception: Abandoned Imperative of the 21st Century (Fort Leavenworth: USA Command and General Staff College, 1997), 8.
[11] Michael Dewar, The Art of Deception In Warfare, New York, Sterling, 1989, 10.

Speed of Command

> *Real-time information will likely drive parallel, not sequential, planning and real-time, not prearranged, decision making.*
>
> **Joint Vision 2010**

The primary benefit of the common operational picture will be the ability to make rapid decisions. From a deception perspective, however, this speed of command will also generate some profound vulnerabilities. The very speed with which decisions are made will inadvertently *speed the effects of any adversarial deception.* The quest for increased speed will also *require us to barter away key portions of our deliberate intelligence cycle* (our traditional deception screen), and finally *speed will translate into predictability* (a key deception target) as automation and standardization will come to dominate our decision making process.

Speed of Deception--Clausewitz largely discounts deception's effectiveness due to the difficulty in getting the deceived to react to the deception within a given time frame. He presumed that it was too hard to prevent the deceived from analyzing the deception effort (given adequate time) to uncover its actual intended purpose.[12] Network-centric warfare's speed would have made a D&D believer out of Clausewitz. Not only will the deceived react almost immediately to deception but the time required to see through deception will no longer exist. Conceivably, deception will enter our shared perception near real-time as soon as our sensors pick it up.

Speed vs. Analysis--Most proponents of network-centric warfare argue that in order to achieve ultimate speed, information must enter the common operational picture near real-time (if not real-time).[13] The sentiment seems to be that if input cannot be automated, we do not need it. Many aspects of intelligence will fall into the category

[12] Carl Von Clausewitz, On War, indexed ed. (Princetown: Princetown, 1984), 203.
[13] VADM Arthur Cebrowski and John Garstka, "Network-Centric Warfare--Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 32.

of 'too slow - must go.' Most raw information will be directly pumped into the common operating picture without evaluation--and without D&D screening. The one filter (in-depth analysis) that might ferret out D&D will itself be locked out due to speed considerations. A blistering optempo will hardly provide the commander time to think, let alone time to turn to ask his intelligence officer for an assessment. The intelligence officers, if they haven't already been downsized out of the staff, will likely be preoccupied anyway with maintaining the common operating picture.

Say an adversary leaks some misinformation into our tactical HUMINT channels and also passes the same misinformation along a communications channel that he feels we are monitoring. This misinformation will enter the automated common operational picture through two of our sensors, which would potentially click a reliable flag next to the misinformation on the operational picture. It would also simultaneously click an unreliable flag up next to conflicting information that was only obtaining through a single unsubstantiated source.

Without the analytical interface, network-centric warfare could conceivably be manipulated by a resourceful opponent. A well trained and experienced analytical capability will offer a depth of understanding about the enemy that will be able to identify potential D&D measures far more effectively than an automated software program. D&D, and thereby its identification, is a creative art not an exact science. As we matrix and chart the battlespace, we will likely be attempting to quantify the data into logical categories; without analytical input, D&D warnings may automatically fall out as rounding errors.

Predictability of Perfection--As our operational art is improved through network-centric's networked common operating picture (standardized no doubt by future doctrine), we stand to lose some of our characteristic unpredictability. Network-centric will require the operator to synchronize based on across-the-board procedures and networks.[14] The predictability of this connectivity provides the enemy the background he needs to tailor D&D measures against us.

During training exercises, some U.S. Army units consistently fall well short in seeing through enemy D&D and rarely use D&D against the opposing force.[15] Some believe D&D is a lost operational art throughout the services;[16,17] in which case it is easy to explain our vulnerability to D&D as we mirror image our opponents. Network-centric warfare may serve to only further distance our decision-makers from the possibilities of D&D. Our network-supported picture, by "clarifying" options, is likely to encourage operational commanders to select the least risky, most favorable and most obvious course of action. The natural tendency (unless compensated for) will be to mirror image this rationality upon our enemy -- effectively blinding ourselves to possible deceptive enemy courses of action.

Our predictability will only help the enemy pin point our D&D vulnerabilities. Additional automation will only further distance our final decisions from the imprecise but unpredictable nature that has historically so often kept our enemies guessing about our intentions and assumptions.

To increase our predictability vulnerability further, the trend is for our methods and sources to become known in this new world of shared intelligence. This increasing transparency will only further enemy D&D capability as knowledge of our collection ability will allow them to D&D target certain key sensors. This is not to say that we should abandon all logical process in favor of total enemy confusion, but the more precisely we formulate decisions based on automatic OODA loops, the easier it will

[14] Ibid, 30.
[15] Bradley Nelson, Battlefield Deception: Abandoned Imperative of the 21st Century (Fort Leavenworth: USA Command and General Staff College, 1997), 21.
[16] Ibid, 1-37.
[17] Smith Douglas, Military Deception and Operational Art (Newport: Naval War College, 1993), 1.

become for a deceiver to identify and employ the D&D measures necessary to channel our decisions. Our doctrine illuminates our weaknesses and strengths to our enemies and us -- it has become increasingly easy to get inside our heads (a key facet of the art of deception).[18]

Self-synchronization

Network-centric's enhanced system integration and its resultant shared perceptions will allow for the control of conflict at lower and lower echelons. This is a positive trend in that it will allow for increased initiative at the small unit level encouraging independent planning, coordination, and maneuver (self-synchronization). The danger, however, is that important operational decisions will be made at the tactical level under intense time constraints and without the benefit of analytical input. At all levels, the increased optempo will generate an environment marked by high stress levels and a demand for quick decisions.

Network-centric's goal of eliminating intermediate staffs will also rob the tactical decision maker of the helpful side of oversight and further diminish the analytical manpower in his nearby chain of command. Again, the intense pressure to maintain aggressive speed and the lack of resident analytical insight will leave the tactical and operational commander wide open to well placed enemy D&D.

Less platforms, more networks

Connectivity is set to replace numerical superiority. Network-centric warfare is being designed for far fewer platforms with greatly improved interface with each other and their environment. The perception seems to be that with highly sophisticated sensor grids and overall informational superiority, our engagement grids (our shooters) can afford to be thin because their firepower will be force multiplied by connectivity. This is where D&D, even if only partially successful, will make its money. If an adversary can

[18] Michael Handel, Mil Deception in Peace and War, (Jerusalem: Magnes, 1985), 26.

feed misinformation into our sensor grids and somehow manipulate our shared operational picture, the result of any misdirected action on our part could be far more destructive than if we possessed numerical superiority as well as technical superiority.

<u>'Lock-out' or Underestimation</u>

Pretend inferiority and encourage his arrogance.

Sun Tzu

Our information superiority may very well breed a superiority complex that would not only lock out enemy options but would also lock out our appreciation for enemy D&D. Deception doesn't require advanced technology - it targets the decision maker, not advanced networks. A primary tenant of Information Warfare is protection, but the primary emphasis is on system protection. Will our future decision-makers, relying on the technical sanctity of our networks, underestimate an innovative enemy's D&D ability? Through the use of D&D, an adversary could effectively hide both critical strengths and critical weaknesses from us and may even be able to obscure his tactical or operational level Center of Gravity. An adversary may use D&D as a force multiplier or as a method of protecting an asymmetrical advantage. More ominously, an opponent may engage in D&D to protect and effectively use a weapons of mass destruction (WMD) capability.

IV. Potential Ability of Informational Superiority to overcome D&D

The future D&D threat is serious, as discussed above, but the same technology that makes network-centric warfare a formidable force multiplier will help to provide many of the counter measures to future D&D. Continued development of a D&D sensitive sensor grid that utilizes multispectural sensing and automated target recognition will help greatly. But as we've seen above, D&D is capable of developing ways to counter our sensors, so it is imperative that we go beyond a purely technical solution.

The oldest and most effective counter to D&D will remain a deep understanding of the enemy through the intelligence cycle; the urge to abandon the analytical process in order to further enhance optempo must be tempered by this realization. Better sensors combined with deeper levels of analysis (enhanced by IT) will provide strong anti-deception tools to the operational decisionmaker as long as the proper understanding of the D&D threat is manifest in our service and joint doctrine/training.

Role of Networked Analysis

Network-centric warfare will demand a streamlined intelligence cycle. In order to ensure that the streamlining doesn't mean the loss of in-depth analysis, the Intelligence Community (IC) must keep pace with the warfighting community's IT RMA. The IC must be able to mold itself as a cohesive whole into an informational node that feeds directly into the network-centric operational picture.

An example of the required virtual integration is already being pursued by the Defense Intelligence Agency (DIA) in conjunction with the rest of the IC through the Joint Intelligence Virtual Architecture (JIVA). JIVA is working towards transparent, virtual, and seamless electronic connectivity between national, operational, and tactical levels in support of both decision-makers and warfighters. Advanced knowledge-based tools as part of JIVA will provide information visualization/presentation, analysis, multisource information fusion, information management, and terminus delivery techniques. Combined with high-capacity communications and advanced databases, JIVA will facilitate real-time predictive analysis and virtual collaboration with multiple IC and warfighter users. [19] The IC must be able to adapt through initiatives like JIVA if it is going to be able to stay abreast of IT RMA's like network-centric warfare. Near real-time analysis and virtual collaboration will go a long ways towards lessening the

[19] Vector 21: A Strategic Plan for the Defense Intelligence Agency, Washington, 1997, 20.

threat of surprise as the result of enemy D&D.

Doctrine

Doctrine provides an official framework for development, training, and future employment. As doctrine can chart the course for modernization and education/training, anti-D&D should be included. A review of the Joint Publications reveals an almost total absence of doctrine on countering adversarial D&D. Even the concept of "counterdeception" as defined by the JCS dictionary does not include identifying foreign deception operations--the term simply refers to the effort to gain advantage from a foreign deception operation.[20]

Operational doctrine does recognize the need for countering enemy D&D, but confines itself to referring to the need for intelligence to provide analysis on this threat.[21] This reference would lead one to believe that the topic would be thoroughly covered in JP 2.0, Joint Doctrine for Intelligence Support to the Operational Commander; however, this pub only devotes one paragraph to the function. This paragraph simply advocates the use of multiple sources and the training of analysts in perceiving deception as measures to avoid adversarial deception. [22] NDP2 seconds JP 2.0 but gives little more in the way of details.[23]

About another 75 joint and service pubs talk about deceptive operations, including JP 3-58, Joint Doctrine for Military Deception, but not one of them mention how we should go about identifying and countering enemy D&D. As the ultimate sign of a lack

[20] Joint Chiefs of Staff, DoD Dictionary of Military and Associated Terms (Joint Pub 1-02)(Washington: March 23, 1994), 118.

[21] Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3.0) (Washington, D.C.: February 1, 1995), III-13.

[22] Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to the Operational Commander (Joint Pub 2.0) (Washington, D.C.: May 5, 1995, III-5.

[23] Naval Doctrine Publication 2, Naval Intelligence (NDP2), (Washington, D.C.: undated), 8.

of emphasis on this important topic, the Universal Joint Task List is also devoid of deception identification/countermeasure focus areas.

Who specifically is responsible for anti-D&D other than the J2? Based on the sparsity of doctrinal references to this function, is it likely that the function will be neglected in the heat of battlespace preparation? Perhaps as a bridge from the J2 to J3, doctrine should call for an expanded defensive IW/C2W role that covers anti-D&D. Currently defensive IW/C2W does not include a D&D counter role. Joint Doctrine for Command and Control Warfare (C2W) (Joint Pub 3-13.1) only mentions countering D&D when it mentions that the IC will need to train for the role.[24] No specific defensive responsibility is given to the C2W cell that would work for the JFC. A dedicated anti-D&D position on the JFC's C2W might serve to heighten D&D awareness and keep the responsibility for the threat from falling between the J3 and J2. As D&D is targeted at C2, it seems logical for C2W to take a more active part in D&D defense (with the J2 as the primary supporting player).

V. Conclusion

While the lure of great leaps forward in information technology draws the U.S. warfighter away from restraint, potential adversaries may well look back to traditional D&D as an important factor in any future conflict. This paper provided fodder for thought on the asymmetrical challenges new IT RMA-based concepts like network-centric warfare may face on the future battlespace. As we forge ahead of all, we run the risk of losing sight of the competition. With the help of consistently powerful sensor denial technology, traditional denial and operational deception may very well be used by weaker and less advanced opponents in the future as an asymmetrical strength to counter

[24] Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W) (Joint Pub 3-13.1) (Washington, D.C.: February 7, 1996), III-6/8.

our IT RMA strength.

This paper focused on the main attributes of one of the very promising IT RMA concepts--network-centric warfare. We explored how placing enormous faith on a sensor grid produced serious D&D vulnerabilities. Given our sensor grid D&D weaknesses, network-centric's overarching informational superiority was shown to actually facilitate the enemy's deception through real-time, common perception altering through the operating picture. Network-centric's speed of command strength was identified as a possible adversarial solution for the traditional difficulty of making deception work at the proper time. Self-synchronization, the reduction in the number of platforms, and our goal of 'locking-out' were all network-centric traits that we demonstrated may leave the U.S. decisionmaker more vulnerable to destructive enemy D&D.

The prognosis, however, doesn't have to be bleak. IT RMA concepts like network-centric warfare will likely evolve with increasingly effective anti-D&D attributes. But visionaries must take time out in this early developmental stage to make sure that the intelligence community will be ready to support their concepts with effective anti-D&D analysis that can be supplied with near-real time tempo. Doctrine must also reflect a clear understanding of anti-D&D methodologies so that future operational commanders are aware of and can plan how to counter D&D when they face it.

Bibliography

Barnett, Roger W. "The Seven Deadly Sins of Network-Centric Warfare," U.S. Naval Institute Proceedings, Jan 1999.

Cebrowski, VADM Arthur K, and Garstka, John J., "Network-Centric Warfare--Its Origin and Future," U.S. Naval Institute Proceedings, Jan 1998, 28-35 .

Clausewitz, Carl von. On War. Eds., Michael Howard and Peter Paret, Princeton, New Jersey: Princeton University Press, 1984.

Deception Maxims: Fact and Folklore. Deception Research Program, Everest Consulting Associates, Princeton Junction, New Jersey, Office of Research and Development, CIA, Washington, DC, April 1980.

Dewar, Michael. The Art of Deception In Warfare. New York, Sterling, 1989.

Handel, Michael I. Military Deception in Peace and War. Jerusalem: Magnes, 1985.

Handel, Michael I. Sun Tzu and Clausewitz. Carlisle Barracks: U.S. Army War College, 1991.

Libicki, Martin C. "Informational Dominance," Strategic Forum, Dec 1997.

Naval Doctrine Publication 2, Naval Intelligecene (NDP2). Washington, undated.

Nelson, Bradley. Battlefield Deception: Abandoned Imperative of the 21st Century, U.S. Army Command and General Staff College, School of Advanced Military Studies, Fort Leavenworth, Kansas, 1997.

Savoie, Thomas A. Deception at the Operational Level of War, U.S. Army Command and General Staff College, School of Advanced Military Studies, Fort Leavenworth, Kansas, 1986.

Smith, Douglas V. Military Deception and Operational Art, Naval War College, Newport, Rhode Island, 1992.

Tzu, Sun. The Art of War. Translated by Ralph Sawyer. Boulder: Westview Press, 1994.

U.S., Joint Chiefs of Staff. DoD Dictionary of Military and Associated Terms. (Joint Pub 1-02) Washington: 1994.

U.S., Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W). (JP 3-13.1) (Washington: 1996), III-6/8.

U.S., Joint Chiefs of Staff. Joint Doctrine for Military Deception JP 3-58. Washington, 1996.

U.S. Joint Chiefs of Staff, Joint Doctrine for Operations (Joint Pub 3.0). Washington, 1995.

U.S. Joint Chiefs of Staff. Joint Doctrine for Intelligence Support to the Operational Commander (Joint Pub 2.0). Washington, 1995.

U.S., Joint Chiefs of Staff (J-6). The Emerging Joint Strategy for Information Superiority. Washington, 1998.

U.S., Joint Chiefs of Staff . Universal Joint Task List Ver 3.0. Washington, 1996.

U.S., Joint Chiefs of Staff. Joint Vision 2010. Washington, 1995.

Vector 21. Defense Intelligence Agency, Washington, 1997.

Vego, Milan. On Operational Art-Third Draft. Newport: Naval War College, 1998.

Zulkifli, Iriani. "Company Profile: Barracuda Technologies AB," Asian Defense Journal, Apr 1998.